



03 - 06 - 00

BIENSTOCK & CLARK
A Partnership Including Professional Associations
FIRST UNION FINANCIAL CENTER
SUITE 3160
200 SOUTH BISCAYNE BOULEVARD
MIAMI, FLORIDA 33131-2367
(305) 373-1100
TELECOPIER (305) 358-1226



March 2, 2000

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Transmitted herewith for filing are papers related to the patent application of:

Inventor(s): ISRAEL DANIEL SULTAN

For: NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA
NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE
PORT ADDRESSES

The filing fee for the enclosed patent application has been calculated as shown below:

	Small Entity				Other than Small Entity	
	No. Filed	No. Extra	Rate	Fee	Rate	Fee
Basic Fee				\$380		\$760
Total Claims	12 - 20 =	0	x9 =		x18 =	
Ind. Claims	3 - 3 =	0	x39 =		x78 =	
____ Multiple claims presented			x130 =		x260 =	
				Total \$380	Total	\$

Check No. 14511 in the amount of \$420.00 is enclosed to cover the filing fee (plus applicable Assignment recording fee).

Respectfully submitted,
BIENSTOCK & CLARK

By

Michael C. Cesarano

Michael C. Cesarano

Reg. No. 31,817

PATENTS

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of ISRAEL DANIEL SULTAN

Serial No.

Filed:

For: NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA
NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE
PORT ADDRESSES

TRANSMITTAL AND CERTIFICATE OF EXPRESS MAILING

Box New Application
Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

I HEREBY CERTIFY that the below listed documents are being deposited with the United States Postal Service "Express Mail Post Office to Address," Mailing Label No. EE598519516 US, under 37 C.F.R. 1.10 on March 2, 2000 and are addressed to Box New Application, Commissioner of Patents and Trademarks, Washington, D.C. 20231.

- ☒ Patent Application (35 pgs.; 12 clms.)
- ☒ Declaration (2 pgs)
- ☒ Small Entity Form - Independent Inventor (1 pg.)
- ☒ Assignment w/Assignment Cover Sheet (5 pgs.)
- ☒ Eleven (11) sheets of informal drawings
- ☒ Fee Calculation Letter (1 pg.)
- ☒ Check No. 14511 in the amount of \$420.00 (covers Assignment fee)
- ☒ Return receipt postcard.

Respectfully submitted,

By Vivian Guerra
Vivian Guerra

By Michael C. Cesarano
Michael C. Cesarano
Reg. No. 31,817
Bienstock & Clark
200 South Biscayne Blvd., Ste. 3160
Miami, Florida 33131
(305) 373-1100

Applicant or Patentee: ISRAEL DANIEL SULTAN

Serial or Patent No.: _____

Filed or Issued: _____

For: NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE PORT ADDRESSES**VERIFIED STATEMENT (DECLARATION) CLAIMING SMALL ENTITY STATUS
(37 C.F.R. 1.9(f) and 1.27(b)-INDEPENDENT INVENTOR)**

As a below named inventor, I hereby declare that I qualify as an independent inventor as defined in 37 C.F.R. 1.9(c) for purposes of paying reduced fees under section 41(a) and (b) of Title 35, United States Code, to the Patent and Trademark Office with regard to the invention entitled: NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE PORT ADDRESSES

described in ☒ the specification filed herewith
☐ application serial no. _____, filed _____
☐ patent no. _____, issued _____

I have not assigned, granted conveyed or licensed and am under no obligation under contract or law to assign, grant, convey or license, any rights in the invention to any person who could not be classified as an independent invention under 37 C.F.R. 1.9(c) if that person had made the invention, or to any concern which would not qualify as a small business concern under 37 C.F.R. 1.9(d) or a nonprofit organization under 37 C.F.R. 1.9(e).

Each person, concern or organization to which I have assigned, granted, conveyed, or licensed or am under an obligation under contract or law to assign, grant, convey, or license any rights in the invention is listed below:

☐ no such person, concern, or organization
☒ persons, concerns or organizations listed below*

*NOTE: separate verified statements are required from each person, concern or organization having rights to the invention averring to their status as small entities. (37 C.F.R. 1.27)

NAME Nexland, Inc.ADDRESS 20801 Biscayne Boulevard, Suite 403, Miami, Florida 33180
☐ INDIVIDUAL ☒ SMALL BUSINESS CONCERN ☐ NONPROFIT ORGANIZATION

NAME _____

ADDRESS _____

☐ INDIVIDUAL ☐ SMALL BUSINESS CONCERN ☐ NONPROFIT ORGANIZATION

I acknowledge the duty to file, in this application or patent, notification of any change in status resulting in loss of entitlement to small entity status prior to paying, or at the time of paying, the earliest of the issue fee or any maintenance fee due after the date on which status as a small entity is no longer appropriate. (37 C.F.R. 1.28(b))

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under section 1001 of Title 18 of the United States Code, and that such willful false statements may jeopardize the validity of the application, any patent issuing thereon, or any patent to which this verified statement is directed.

ISRAEL DANIEL SULTAN

NAME OF INVENTOR

NAME OF INVENTOR

NAME OF INVENTOR

Signature of Inventor

Signature of Inventor

Signature of Inventor

Date

Date

Date

/ 03/01/2000

NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE PORT ADDRESSES

BACKGROUND

Virtual private networking (VPN) using TCP/IP enables secure, high speed communications between remote computing sites, using the internet as a communications medium. Information passing between sites across the internet may be protected against interception by unwanted eavesdroppers or malicious hackers by a variety of security measures. Effective security measures must, at a minimum, incorporate functions that ensure any or all of the following protections: Data integrity against the inadvertent or malicious modification of data during transit; prevention against denial-of-service attacks by employing anti-repeat measures; source authentication; confidentiality of source address and other header information during transit; and packet payload protection against unwanted interception. One standard model for providing internet security is the Internet Protocol Security suite, IPSec. IPSec works with the TCP/IP communications protocol to provide secure communications between devices connected to the internet or connected to private LANs (Local Area Networks) that are, themselves, connected to the internet.

The TCP/IP (Transmission Control Protocol/Internet Protocol) protocol suite uses IP addresses to identify each device on a network. A global IP address uniquely identifies a device on the internet. Such devices may be computers, printers, routers, switches, gateways, or other network devices. Devices having global IP addresses may be directly referenced as a source or destination on the internet. The TCP/IP communications protocol, however, is not exclusively limited to the internet, but may be used on private LANs as well. Private LANs using TCP/IP frequently use "local" IP addresses for network devices. Although no two devices on a private LAN may share the same local IP address,

private LANs are isolated from the internet, and local devices on the LAN are not visible from the internet. IP addresses for local devices therefore need not be “globally” unique. A LAN using local IP addresses will be connected to the internet through a gateway, which is a device that may filter or route messages between the LAN and the internet. Since the gateway is directly attached to the internet, and is visible to it, the gateway must have a globally unique IP address for communicating across the internet. However, since the LAN is not directly visible from the internet, local machines on the LAN do not require IP addresses that are globally unique.

TCP/IP is the communications protocol that is used on the internet. Information to be communicated using TCP/IP is contained in “datagrams.” A datagram consists of a discrete “packet” of information to which one or more headers are appended. Headers contain information needed by TCP/IP to direct the packet to its intended destination and to ensure its proper handling during transit. Each datagram is individually addressable, and may be a connection-oriented TCP datagram or a “connectionless” UDP (User Datagram Protocol) datagram. Each UDP datagram includes an IP header and a UDP header. The IP header contains at least a “source” IP address and a “destination” IP address, while the UDP header includes source and destination service addresses (port addresses, given as numbers). In IPv4, IP addresses are 32 bits in length, and are associated with the now-familiar xxx.xxx.xxx.xxx format. In this format, each three-digit segment is a binary octet representing a number between 0 and 255. A complete IP address combines the address of a logical network or network segment with the address of a “node” (device) on the network. The address of the network or network segment may encompass the first 3, 6, or 9 digits of the IP address. A device on the network or network

segment is identified by a node address that consists of those remaining digits that are not used in the network or network segment address.

The source and destination service addresses contained in a UDP header are 16-bit numbers, variously known as “ports” or “sockets,” which are used to direct the packet to an intended process that is active on the sending or receiving device. The term “port,” or “port address,” as used herein, refers to a service address field in a UDP header. Although in theory there are as many ports as there are addresses in a 16-bit number, by convention many port addresses have been reserved for established processes. Thus, for example, port 80 is reserved for HTTP, and ports 20 and 21 are reserved for FTP. Through the use of port addresses, data arriving at a local machine running more than one process will be directed to the process for which it was intended. Where a process running on a local host is not one of the reserved processes, the local host may select any port number from a pool of unreserved port numbers to identify the “source” process. A reply packet referencing that port number in the “destination” field will be directed to the process.

With the explosive growth of internet usage during the last decade, and its projected growth in the future, globally unique IP addresses have become a scarce resource. In addition, many businesses maintaining private LANs have little or no need for each computer and device on the LAN to have a unique global IP address. Many such businesses would, in any event, prefer to maintain the confidentiality of their computers’ IP addresses. Rather than waste limited global resources by giving each local device a unique global IP address, many private LANs utilize local IP addresses for devices on the LAN. In order to provide connectivity to the internet, such LANs will employ a single

globally unique address to be used on the internet by the gateway separating the LAN from the internet.

Through the use of Network Address Translation (NAT) techniques, a gateway device separating a LAN from the internet can provide security as a firewall while enabling machines with local IP addresses to access the internet through the unique global address of the gateway. A device on a LAN may have a static local IP address, or it may have a local IP address dynamically assigned to it at log on. The gateway maintains a translation table with the local IP addresses for each device on the LAN. A UDP packet sent from a local machine and destined for the internet will have its local IP address and port address identified in the source fields of the IP and UDP headers, respectively. The gateway will receive the packet from the local machine, will substitute its external globally-unique IP address and a new port address (taken from a pool of unused, unreserved port addresses) into the source fields of the IP and UDP headers. It will next update the CRC (Cyclical Redundancy Check) and make any other necessary changes to ensure data integrity, then will send the packet to the internet. As part of the process, the gateway will update its internal translation table to cross reference the local machine's IP address with the source port address originally reported by that machine, with the new source port address assigned to the internet-bound packet, and with the destination IP address. Upon receipt of a reply from the internet, the gateway will recognize its own IP address in the packet header, and will examine the incoming packet's destination port address. If it finds the destination port address in its internal table, the gateway will substitute the cross referenced local machine's IP address and original port address into the destination fields of the packet, will update the CRC and any other necessary parameters, and then will

1 dispatch the packet to the LAN, where it will be received by the local machine and directed
2 to the appropriate process. In this manner, a number of computers on a LAN having only
3 local IP addresses can communicate across the internet through a single globally unique
4 IP address.

5 Although NAT gateways provide firewall security against direct accessing of the LAN
6 from the internet, they do not provide security against interception or modification of a
7 packet intended for the LAN while in transit on the internet, and they do not ensure
8 "trustworthiness" from challenges originating within the LAN. Thus, the security provided
9 by IPSec is a necessary protection for LANs that must maintain security while interfacing
10 with the internet.

11 A common implementation of IPSec is to provide security for VPNs consisting of at
12 least one main computing site and one or more remote LANs. The main site and remote
13 LANs are connected across the internet, using that high speed medium to communicate
14 between sites instead of significantly more expensive private leased lines. The drawback
15 to using the internet as a transmission medium, however, is that the internet is inherently
16 insecure, and provides little or no inherent protection against the snooping, detection,
17 "spoofing," or ultimate theft, modification or diversion of messages by hackers. Thus, there
18 is a need for comprehensive security measures where secure data transmissions are
19 required. The IPSec protocol implements security measures to ensure authentication of
20 data and data integrity.

21 The IPSec protocol suite implements security at the network layer of the multi-
22 layered OSI (Open Systems Interconnection) network reference model. The suite includes
23 a number of separate protocols that are used in conjunction with one another to ensure the

1 security of UDP datagrams that carry information across the internet. The base
2 architecture of IPSec compliant systems is explained in RFC2401, "Security Architecture
3 for the Internet Protocol," S. Kent and R. Atkinson (November 1998). The AH
4 (Authentication Header) protocol assures data integrity, source authentication, and
5 incorporates "anti-repeat" measures to deter denial-of-service attacks. ESP (Encapsulation
6 Security Payload) protocol provides protections similar to AH, but adds the additional
7 feature of payload encryption. Both AH and ESP headers have a field for a Security
8 Parameters Index (SPI). The SPI is a 32-bit pseudo-random value that is used to identify
9 a Security Association (SA) for the datagram. Further information regarding these
10 protocols may be found in RFC1826, "IP Authentication Header," by R. Atkinson (August
11 1995), and RFC2406, "IP Encapsulating Security Payload (ESP)," S. Kent and R. Atkinson
12 (November 1998). ISAKMP/Oakley (Internet Security Association and Key Management
13 Protocol, also commonly referred to as Internet Key Exchange – IKE) is a handshaking
14 protocol that establishes the parameters for a secure session between two hosts and
15 provides for the exchange of keying and other security information that is used to
16 implement the secure session and permit the transmission of encrypted data. The
17 ISAKMP/Oakley protocol (hereafter referred to simply as ISAKMP) involves the initial
18 exchanges of unencrypted messages to provide both machines with initialization data from
19 which authentication may be established and secure keys for data encryption may be
20 generated. An explanation of these processes may be found in RFC2409, "The Internet
21 Key Exchange," D. Harkins and D. Carrel (November, 1998). Once security parameters
22 sufficient establish Security Associations (SAs) between hosts have been exchanged, all
23 subsequent transmissions will be encrypted and fully authenticated in accordance with the

1 agreed-upon protocols. At that point the ISAKMP protocol terminates. Subsequent
2 addressing is based upon the IP address for each machine and the machine's SPI for that
3 session. The SPI is unique for each machine during a session. The gateway for a private
4 LAN will maintain an internal table in which "SPI-in" is a value that is cross referenced to
5 the local machine's IP address, and "SPI-out" is cross referenced to the IP address of the
6 machine on the internet that is communicating with the local machine. The SPI for each
7 machine is computed from information exchanged during the ISAKMP transmissions, and
8 is carried in the AH or ESP header that is appended to UDP packets. Because IPsec
9 protocols may be nested to provide security in a variety of environments, a single datagram
10 may include both an AH and an ESP header, and may encrypt some header information.

11 Each of the foregoing security protocols modifies the UDP packet by placing new
12 header information on the packet, modifying certain fields within the packet to conform to
13 the protocol being used and, in some cases, encrypting the payload and all or parts of
14 other packet headers. Thus, under IPsec, when a UDP datagram leaves a "secure"
15 domain for transit across an untrusted network, it will normally consist of an IP header, an
16 AH or ESP header (or both), and an encapsulated payload. Header information will include
17 a destination address, an SPI, and sufficient SA information to ensure that the datagram
18 reaches its destination and can be authenticated to the destination host. Encapsulation
19 of the payload ensures that information contained within the payload is denied to unwanted
20 eavesdroppers and hackers. The initial destination host for the datagram may be a router,
21 gateway, or firewall between a LAN and the internet. Upon arrival at the device on the
22 border between the LAN and the internet, the datagram may be opened, examined or

1 decrypted in whole or in part, analyzed for further address information, and routed to a
2 local IP address on the LAN.

3 The ISAKMP handshaking protocol used in IPSec requires that both hosts intending
4 to establish a secure session between them use a process-specific port address (Port 500)
5 for initial message exchanges. For this reason, Port 500 has been assigned for exclusive
6 use with the ISAKMP protocol. By convention, computers attempting to negotiate secure
7 communications parameters by employing the ISAKMP protocol must communicate strictly
8 through each computer's Port 500. That is, ISAKMP messages from either computer must
9 identify Port 500 as both the source and destination port addresses. If either computer
10 receives a packet in which Port 500 is not specified as being both the source and
11 destination, the packet will be discarded.

12 While this protocol provides assurance that two hosts are communicating with each
13 other, it becomes unworkable when one host is located on a LAN that uses local IP
14 addresses and a NAT gateway. For example, Host A, having a local IP address on a
15 remote LAN protected by a NAT gateway, wishes to establish a secure session with Host
16 B, located at a main office computing site. Host A would initiate the protocol by sending
17 an unencrypted UDP datagram to Host B, giving the "destination" as Host B's IP address,
18 and the destination port address as "Port 500." However, when the datagram reaches the
19 NAT gateway connecting the remote LAN to the internet, the gateway will translate the
20 destination port address to an arbitrary port number. Upon the arrival of the datagram at
21 Host B, the ISAKMP protocol will not be recognized, and Host B will not respond. The
22 computers will fail to establish a secure session. Because of this difficulty, it has heretofore
23 been believed that the ISAKMP protocol cannot be used to establish a VPN using a NAT

1 gateway where each computer on the remote LAN uses a local rather than a global IP
2 address.

3 It is therefore an object of this invention to provide a gateway that will permit the use
4 of ISAKMP protocol authentication and key exchanges between a computer having a non-
5 global IP address and a host computer, using the internet as a transmission medium.

6 It is a further object of this invention to provide a gateway that will allow any number
7 of computers on a private LAN using local IP addresses to initiate or receive messages via
8 the internet using ISAKMP protocol.

9 It is another object of this invention to provide a method for employing virtual private
10 networking between two or more LAN sites on the internet, using ISAKMP protocol to
11 initiate secure communications.

12 These and other objects of the invention will become apparent throughout the
13 following description.

14 **SUMMARY OF THE INVENTION**

15 In accordance with the present invention, a computer using a local IP address on
16 a remote LAN attached to an external network such as the internet through a NAT gateway
17 will use the ISAKMP protocol to exchange keys and establish SAs that will support a
18 secure session under IPSec. For non-ISAKMP traffic, the gateway performs address
19 translation as normal. However, whenever a machine on the LAN originates an ISAKMP
20 protocol message, the gateway will identify the datagram containing port addresses of Port
21 500. Upon encountering such a datagram, the gateway will translate the source IP
22 address, but will not translate the source port address, leaving it at Port 500, and will
23 dispatch the packet to the internet with Port 500 designated as both the source and

1 destination port addresses. The gateway will also update its internal table to "bind" Port
2 500 to the local IP address and associate that binding with the external IP address of the
3 destination machine for a predetermined length of time. If a valid reply is not received
4 within the predetermined length of time, the "binding" between Port 500 and the local IP
5 address will be released. This feature is necessary to ensure that Port 500 is not tied-up
6 indefinitely, such as, for example, in a situation in which an ISAKMP protocol transmission
7 has been initiated to an incorrect destination IP address. Under those conditions, the
8 gateway would never receive a valid reply. If there were no timer to release Port 500 after
9 a period during which a valid reply is not received, the port would remain bound to the local
10 IP address until the gateway was reset. For most conditions, a period of two seconds
11 should be a sufficient length of time to maintain the binding between Port 500 and the local
12 IP address while awaiting a valid reply.

13 During the time that Port 500 is bound to a local IP address, the gateway will
14 continue normal datagram processing of datagrams not having Port 500 port addresses
15 while awaiting a valid reply. A valid reply will be a datagram having a source IP address
16 that is the same as the external IP address that is associated with Port 500, and will have
17 both the source and destination port addresses as Port 500. While awaiting a valid reply,
18 the gateway will ignore other UDP datagrams from the external network having Port 500
19 source and destination port addresses, but not the proper source IP address. Also, while
20 Port 500 is bound to a local IP address, datagrams received from the LAN having source
21 and destination port addresses of Port 500 will undergo "normal" address translation in
22 which the Port 500 source port address will be translated to an arbitrary, unused port
23 address before being sent to the external network. Because such a datagram does not

1 have both a source and destination port address of Port 500, it is not a valid ISAKMP
2 datagram, and will be ignored upon reaching its IP destination. If the period of binding Port
3 500 to a local IP address should expire without a valid datagram having been received by
4 the gateway, the binding will be released, and Port 500 will become available for use by
5 the next datagram having a Port 500 source and destination port address.

6 While Port 500 is bound, upon receiving a valid reply datagram having source and
7 destination port addresses of Port 500 and the correct source IP address, the gateway will
8 process the datagram by substituting the IP address of the local machine into the datagram
9 header's destination IP address field, then will pass the datagram through to the LAN for
10 delivery to the local machine. When the datagram leaves the gateway, the gateway will
11 release the binding between the local IP address and Port 500, and will resume normal
12 datagram processing.

13 If a reply having the proper source IP address and port addresses of Port 500 is not
14 received from the external network, the gateway will time-out after a short predetermined
15 length of time. If the gateway should time-out before a valid reply is received, that ISAKMP
16 message exchange cannot be completed, but must be re-initiated.

17 Once the ISAKMP protocol has been completed, and an encrypted secure session
18 is under way, the gateway will perform local address translations by referencing the SPI
19 in the ESP header of incoming and outgoing datagrams. The gateway will also ensure that
20 each packet type (type 50 for an ESP packet) is correct for the datagram being passed
21 through the gateway. Occasionally, a secure session across a VPN will be interrupted, or
22 a new session started. The gateway's first indication of this will be its receipt of a type 50
23 datagram in which the IP addresses are recognized but the SPI associated with the

1 destination does not appear in its internal table. When this happens, the gateway will
2 dispatch the datagram to the destination IP address using the new SPI, and will also set
3 the destination SPI value (SPI-in or SPI-out, depending upon the direction of the
4 transmission) in its table to the new value, and the source's SPI value to zero. Upon
5 receiving a reply to the transmission, the gateway will replace the zero in the SPI field table
6 with the new SPI for the destination IP address.

7 Because the gateway of this invention does not encrypt or decrypt messages, but
8 simply passes the payload (which may be encrypted or unencrypted) through to the LAN
9 or to the internet for processing at the receiving machine, it does not require intensive
10 processing functionality, and may be used for private LANs in which expense and simplicity
11 of setup and maintenance are considerations.

12 **A BRIEF DESCRIPTION OF THE DRAWINGS**

13 Further objects and advantages of the present invention can be found in the detailed
14 description of the preferred embodiment when taken in conjunction with the accompanying
15 drawings in which:

16 Figure 1 depicts a virtual private network in which a remote LAN using local IP
17 addresses is networked with a main computing site via an external network which may be
18 the internet. The LAN is connected to the external network through a NAT gateway.

19 Figure 2 depicts a decision chart used by the gateway of this invention to process
20 UDP datagrams received from the LAN for transmission to the internet.

21 Figure 3 depicts a decision chart of steps used by the gateway of this invention to
22 process UDP datagrams received from the internet for delivery to a device on the LAN.

Figure 4 is provided for reference in following the charts shown in Figures 5, 6 and 7. Figure 4 is a table containing IP addresses of local machines on a LAN (L-1 through L-3), the internal and external IP addresses of a gateway, and the IP addresses of external devices ("targets" T-1 through T-3) on an external network.

Figures 5a - 5c show representative fields from an internal table of the gateway cross referencing local IP addresses of machines on a LAN (L-1, L-2, . . . L-x) and external IP addresses of external devices (T-1 through T-3) with SPIs (security parameter indexes) used to authenticate encrypted datagrams. SPI-out represents the SPI of an encrypted datagram leaving the gateway for a device on the internet, while SPI-in represents the SPI of an encrypted datagram destined for a local machine on the LAN. Each view of the table, a, b and c, reflects header values for source, destination, and SPI at different points in time. The changing values signify the commencement of a new session by one a local machine with a target machine.

Figure 6 shows representative fields in datagram headers being exchanged between a single local machine and a single device on the external network. Header values are modified through processing by the gateway of this invention.

Figure 7 shows representative fields in datagram headers being exchanged between three local machines (L-1 through L-3) on a LAN, and three targets (T-1 through T-3) on an external network as they are modified through processing by the gateway of this invention.

Figure 8 is a schematic diagram of signals passing between the datagram processing function and the timer.

DETAILED DESCRIPTION OF THE DRAWINGS

In Figure 1, a virtual private network (VPN) is shown in which a private local area network (LAN) 10 is connected to a computing site 30 located on the internet 50. The LAN 10 uses local IP addresses, and is connected to the internet through the network address translation (NAT) gateway of this invention 20. The computing site 30 may be a business headquarters, or one of any number of private LANs used by a multinational corporation, an educational facility, or any other site which will be frequently accessed from remote locations. Such sites will normally have a firewall or gateway 35 capable of running encryption and other security applications. Such a gateway will have the ability to open a packet, decrypt or otherwise access its contents, and perform address translation, routing, de-encapsulation, and data manipulation functions as well. While such devices are able to support ISAKMP and other IPSec protocols, they do so by opening and decrypting packets, and manipulating data, and are, by and large, too expensive and powerful to be employed efficiently at remote LAN sites needing to establish a VPN with the main computing site.

A server 40 at the main site runs the VPN server software. Computers 15 at remote sites each run appropriate VPN client software that implements IPSec security protocols on each computer.

A computer 15 on the LAN 10 will communicate with devices on or across the internet through gateway 20 by sending an IP datagram to a server 40 at the computing site 30.

Datagrams received at the gateway 20 are processed according to the decision charts shown in Figures 2 and 3. Although the flow charts of Figures 2 and 3 show both

1 the processing steps and a sequence for the steps, the order for performing some of the
2 functions is not critical, and some of the steps may be done in an order other than is shown
3 in the flow charts without affecting the ultimate result. For example, Figures 2 and 3 show
4 that the first step after a datagram is received by the gateway is to determine the datagram
5 type, while the last step is to perform the IP address translation that is necessary before
6 the datagram is passed through the gateway. Some embodiments, however, could place
7 the step of address translation to some point earlier in the process, and this would not
8 affect the outcome of the process. Since the order of translating the IP address is not
9 critical to the overall process, the determination of when this translation should be done is
10 a matter of engineering choice.

11 As shown in Figure 2, upon receiving a datagram from the LAN, the gateway will
12 check to see whether the datagram is encrypted. It will do so by checking the "Next
13 Header" field in the IP header to determine the type of datagram it is dealing with, and to
14 see whether the datagram has been encrypted. A datagram type of 50 (ESP) indicates
15 that the datagram is encrypted, and port address information may not be available.

16 Continuing through the decision tree of Figure 2, if the datagram is encrypted, the
17 gateway will check the datagram's SPI to see whether it appears in the SPI-out field of the
18 gateway's internal table. Representative fields from such a table are shown in Figures 5a
19 - 5c. If the SPI of the datagram is found in the SPI-out field of the internal table, the
20 gateway will modify the source IP address of the datagram to be the external IP address
21 of the gateway, and will send the datagram to the external network for delivery to an
22 external device.

1 If the datagram is encrypted, but the SPI does not appear in the gateway's internal
2 table, then according to the decision chart of Figure 2 the gateway will assume that the
3 datagram is initiating a new session. In this case the gateway will set the SPI-in field of its
4 internal table to zero (0) and will set SPI-out to the new SPI from the datagram. These
5 modifications to the internal table are reflected in Figures 5a and 5b, in which a "new" SPI
6 ("14662"), which did not appear in the SPI-out field of the gateway's internal table in Figure
7 5a, is shown as having been entered into the SPI-out field, and SPI-in has been set to zero
8 (0) in Figure 5b. The encrypted datagram will then be sent to the external gateway after
9 the source IP address has been translated from that of the local device to the external IP
10 address of the gateway. These steps are shown in Figures 5b and 5c.

11 Continuing with the decision chart of Figure 2, if the datagram is not encrypted, the
12 gateway will next check the datagram's destination port address. If the port address is
13 anything but Port 500, the gateway will enter the source port address into its internal table,
14 cross reference it with the (local) source IP address, and will then substitute an arbitrary,
15 unused port address into the source port address field of the IP header. It will also enter
16 the new port address in its internal table, again cross referenced to the (local) source IP
17 address. This process, which is used for unencrypted datagrams not having Port 500 as
18 a port address, shall be referred to as "normal address translation" for datagrams
19 originating on the LAN. These translations are shown in Figure 6, rows 1 and 2. The
20 datagram will then be dispatched to the internet for routing to the destination IP address.

21 In Figure 2, where an incoming datagram's source and destination port addresses
22 are Port 500, the gateway must next check its tables to see whether Port 500 is already
23 bound to an IP address. If Port 500 is free, then the gateway will "bind" Port 500 to the

1 (local) source IP address of the datagram, will create an association between the port and
2 the (external) destination IP address, and will send a signal to start the internal timer. The
3 gateway will also process the datagram by substituting the gateway's external IP address
4 for the local IP address in the source IP address field. It will not, however, translate the
5 source port address. By suspending the "normal" translation of the source port address,
6 the gateway ensures that the target machine will be able to recognize the datagram as
7 being an ISAKMP datagram. These steps are also shown in Figure 6, rows 5 and 6.

8 In Figure 2, if an incoming datagram from the LAN has a source and destination port
9 address of Port 500, but Port 500 is already bound to some other local IP address, then
10 the gateway cannot bind Port 500 for the message then being processed. In that event,
11 the gateway will process the datagram "normally," as if it were not an ISAKMP datagram.
12 That is, it will translate the datagram's source port address to an arbitrary number and will
13 translate the source IP address to be that of the gateway's external IP address. The
14 gateway will then send the datagram to the internet, where it will be rejected by the target
15 because it does not conform to an ISAKMP datagram. This event is depicted in Figure 7
16 at rows 15 and 16.

17 In figure 3, a decision chart is shown which outlines the steps the gateway will follow
18 in processing datagrams received from the internet. Upon receiving a datagram, the
19 gateway will first check its type and, if the datagram is encrypted, will check to see whether
20 the SPI appears in its internal table. If the SPI is recognized, its destination IP address will
21 be translated to be the IP address of the local device, and the datagram will be passed to
22 the LAN for delivery to the local device. If the SPI is not recognized, the gateway will next
23 check to see whether its SPI-in field corresponding to the datagram's source IP address

1 is zero (0). If SPI-in is zero, the gateway will assume that the datagram is the first reply of
2 a new session and will replace the zero in the SPI-in field with the SPI of the datagram.
3 The gateway will then translate the destination IP address to be the local IP address of the
4 device on the LAN, and will send the datagram to the LAN for delivery. This event is
5 shown in Figures 5b and 5c. In Figure 5b, the SPI-in for local machine L-1 has been set
6 to zero. Upon the gateway's receipt of a datagram from the internet having an SPI of
7 3288, the gateway will not find that SPI in its SPI-in field. The gateway will next check to
8 see whether the SPI-in field is holding a value of zero. Upon determining that SPI-in for
9 local machine L-1 is zero, the gateway will replace the zero with the SPI of the datagram
10 ("3288") and will send the datagram to the LAN. This is shown in Figure 5c.

11 In Figure 3, if the datagram from the internet is not encrypted, the gateway will
12 check to see whether it has a port address of 500. If it does not, the datagram will undergo
13 "normal" address translation for datagrams from the external network, meaning that the
14 local port address and local IP address of the device on the LAN will be substituted into the
15 destination fields of the datagram, and the datagram will be sent to the LAN for delivery.
16 This "normal" address translation for datagrams from the internet is shown in Figure 6 at
17 rows 3 and 4.

18 Again referring to Figure 3, If the datagram does have a port address of 500, the
19 gateway must next check to see whether Port 500 is bound to a local IP address and is
20 associated with the datagram's (external) source IP address. If it is, then the datagram is
21 valid, and will be passed to the LAN after the destination IP address has been translated
22 from that of the external gateway to the IP address of the local device. Upon passing the

1 datagram to the LAN, the gateway will release Port 500. This event is illustrated in Figure
2 6 at rows 7 and 8.

3 If, in Figure 3, Port 500 is bound to a local IP address, and is associated with an
4 external IP address other than that found in the source IP address of the datagram, then
5 the datagram is not valid and will not be further processed by the gateway. This event may
6 be seen in Figure 7 at rows 25 - 31. At rows 25 and 26, local machine L-1 sends an
7 ISAKMP datagram to target T-1. At this point, Port 500 is bound to the IP address of local
8 machine L-1 and is associated with the IP address of target T-1. However, as shown in
9 Figure 7, the timer "times" out before a reply is received at the gateway from T-1, and, at
10 row 27, Port 500 is released. At rows 28 and 29, local machine L-3 sends an ISAKMP
11 datagram to target T-3, binding Port 500 to L-3's IP address and creating an association
12 with T-3's IP address. While Port 500 is bound, a reply is received from T-1. However,
13 because Port 500 is bound, and is associated with T-3's IP address, the reply from T-1 is
14 discarded. This is shown at rows 30 and 31 of Figure 7.

15 Figures 5a - 5c depict an internal table of the gateway in which the IP addresses
16 and SPI numbers for encrypted communications between local computers and targets on
17 the internet are maintained. Fields for "L-1," "L-2," "L-x," and "T-1" through "T-3" are
18 included for ease of reference, and do not appear in the gateway's internal tables. In
19 Figure 5, the field "SPI-out" holds the SPI for each target machine during a secure session
20 with a specific computer on the LAN. The "SPI-in" field gives the corresponding SPI that
21 will be recognized by the local computer as signifying a valid datagram intended for it.
22 Figure 5a shows the table at a beginning time. Eight (8) local computers have participated
23 in encrypted sessions with three targets, T-1 through T-3 during the life of the table's data.

1 This is shown by the fact that each local machine shows an SPI-in associated with its IP
2 address. Although only three targets are shown in the table, it may be noted that each
3 target is using a different SPI-out for communications with each local machine. In this
4 manner, a target will know from which source an encrypted datagram was generated.

5 Figure 5b shows the same local and target computers as Figure 5a. Here, however,
6 the SPI-out for the session between L-1 and T-1 is a new SPI, indicating a new session
7 between the computers. The gateway's first indication that a new session is taking place
8 is its receipt of an encrypted datagram from the LAN having an SPI – "14662" – that is not
9 in its table. The gateway forwards the datagram to the internet, but also modifies its table
10 to place the new SPI in the SPI-out field associated with the source and destination IP
11 addresses for that datagram. It also places a zero in the SPI-in field as a marker to
12 indicate that a new SPI-in is also expected. Figure 5c shows that a new SPI – "3288" –
13 was included in a datagram received from T-1. That SPI has been entered into the
14 gateway's SPI-in field, and further communications between L-1 and T-1 during this
15 session will use those SPI's to authenticate their messages.

16 Figure 6 charts the flow of representative datagrams through the gateway of this
17 invention by a single computer on a LAN communicating with a remote target on the
18 internet. Each row of the chart represents information in a datagram at either the LAN
19 interface with the gateway or the internet interface with the gateway. Consecutive rows
20 represent data entering the gateway from one side and leaving the gateway at the other.
21 The gateway has one IP address, which may be a local IP address, at its interface with the
22 LAN, and a global IP address at its interface with the internet. The columns in Figure 6
23 depict the side of the gateway the datagram is traversing, the type of datagram, the

1 datagram's source IP address and port address, the datagram's destination IP address
2 and port address, and the datagram's Security Parameter Index (SPI) for encrypted
3 datagrams of type 50, using ESP (Encapsulated Security Payload) protocol.

4 Row 1 of Figure 6 shows a UDP datagram arriving at the local interface of the
5 gateway, and having a source IP address corresponding to local computer L-1, and a
6 destination IP address of the target on the internet, T-1. For ease of reading, Figure 4
7 provides a table of IP addresses cross referenced with local designations L-1 through L-3,
8 and target designations T-1 through T-3. The source port address for L-1 is Port 6404, and
9 the target's destination port is Port 80. Since the datagram is not encrypted, and does not
10 exhibit a port number of 500, it undergoes a normal translation in which an "arbitrary" port
11 address, Port 10425 is substituted into the source port address field and the gateway's
12 external IP address is substituted for the source IP address of the datagram. Although the
13 translated source port address is said to be "arbitrary," it will normally be the next in a
14 sequence taken from a pool of unreserved and presently unused port addresses
15 maintained by the gateway.

16 As the datagram exits the gateway, as shown Figure 6, in row 2, the address
17 translation function of the gateway has substituted the gateway's external IP address into
18 the datagram header for the source IP address, and has given the source port an arbitrary
19 number. Rows 3 and 4 show the reply datagram from the target. In row 3, a UDP
20 datagram from the target shows the destination IP address as being the external IP
21 address of the gateway, and a destination port as being the port address arbitrarily
22 assigned by the gateway. Since the datagram is not encrypted and does not have a port
23 address of 500, the datagram undergoes normal translation of the destination port address

1 and IP address, then is sent to the LAN. In row 4, the gateway has substituted the local
2 computer's local IP address and port address in the destination fields of the header before
3 sending the datagram to the LAN.

4 In row 5 of Figure 6, the local computer initiates an ISAKMP protocol with the target.
5 The datagram type is shown as ISAKMP. Both the source and destination port addresses
6 are Port 500. When the gateway determines that the destination port address is Port 500,
7 it checks to see whether Port 500 is currently bound to any IP address. Since it is not, the
8 gateway passes the datagram, translating only the source IP address field to show the
9 gateway's external IP address, but without changing the source port address.

10 In Figure 6, rows 5 - 16 show the six standard ISAKMP "handshaking" datagram
11 exchanges necessary to establish SAs (Security Associations) to support fully encrypted
12 and authenticated datagrams. Although some modes of ISAKMP use fewer exchanges,
13 the main mode is depicted in Figure 6. Following the establishing of SAs, the local
14 computer and the target begin communicating using ESP protocol encrypted datagrams.
15 Here, datagram validity is maintained through the use of Security Parameter Indexing –
16 SPI – numbers in an SPI field of the datagram's header. Each host recognizes a datagram
17 "addressed" to its SPI, which can be modified during a session by mutual agreement of the
18 hosts as necessary to ensure continued security. When an encrypted datagram passes
19 through the gateway, as depicted at Figure 6, rows 17 and 18, neither the source nor the
20 destination SPI is modified by the gateway, although the datagram's source IP address is
21 translated to be the gateway's external IP address.

22 Thus, when an encrypted datagram is received by the gateway, it will be signified
23 by a datagram of type 50 (ESP). Upon encountering that datagram type, the gateway will

1 check the datagram's Security Parameter Index (SPI) to see whether that SPI is recorded
2 in its internal table. If it is, the gateway will translate the datagram's source or destination
3 IP address, as appropriate, and will send the datagram to the LAN or the internet,
4 depending upon the direction of transmission. However, if the SPI of a datagram from the
5 LAN does not appear in the gateway's internal table, and the source and destination are
6 recognized IP addresses, the gateway will assume that a new session has been started.
7 In this case, it will pass the datagram to the external network leaving the new SPI intact,
8 but recording the new SPI in the "SPI-out" field of its internal table and placing a zero into
9 the "SPI-in" field. At rows 25 and 26 it may be seen that a new SPI has appeared,
10 signifying a new session. This event corresponds to figure 5b, where the "0" in the "SPI-in"
11 field corresponds to the new SPI-out of "14662." At rows 27 and 28, the reply packet from
12 the external network shows that "old" SPI "9802" has been replaced with "new" SPI "3288."

13 Figure 7 is similar to Figure 6, except that it illustrates the passage through the
14 gateway of this invention of datagrams between three computers on a LAN, designated L-
15 1, L-2, and L-3, and three targets on the internet having unique global IP addresses, T-1,
16 T-2 and T-3. In Figure 4, for ease of reference, a table containing the IP addresses of
17 these devices is given. As shown in Figure 7, a transmission designated "L-1 Out"
18 represents a transmission from local computer L-1 to the gateway. "T-1 In" represents a
19 transmission from the gateway to target T-1. "T-1 Out" represents a transmission from
20 target T-1 to the gateway, while "L-1 In" represents a transmission from the gateway to
21 computer L-1.

22 As shown in rows 1-8 of Figure 7, computers L-1 and L-2 conduct "in the clear"
23 communications with targets T-1 and T-2. At row 9, L-1 commences an ISAKMP session

1 with T-1. Rows 9-14 show the first three messages exchanged between L-1 and T-1
2 during the ISAKMP protocol. At row 15, computer L-3 commences an ISAKMP-1 message
3 exchange with T-3. However, at that time Port 500 is bound to L-1 and is associated with
4 the IP address of T-1, awaiting an ISAKMP-4 reply from T-1. In this situation, the datagram
5 from L-3 cannot bind Port 500, and its source port address will be translated. As such, L-3
6 cannot complete the transmission that was started at row 15.

7 Thereafter, at rows 17-18, T-1's reply (ISAKMP-4) is received at the gateway and
8 sent to L-1, and Port 500 immediately becomes available. Thus, when L-3 reattempts its
9 ISAKMP-1 transmission at row 19, the transmission is successful.

10 At rows 19-20 of Figure 7, L-3's ISAKMP-1 transmission binds Port 500 to L-3's IP
11 address. Thus, when L-1 attempts its ISAKMP-5 transmission, at rows 21-22, Port 500 is
12 not available, and the gateway simply translates the destination port address from Port 500
13 to an "arbitrary" port number – in this case, "9063" – and sends the datagram to the
14 internet, where target T-1 will not recognize it as an ISAKMP datagram. However, after L-3
15 releases Port 500, at rows 23-24, L-1's next attempt to send its ISAKMP-5 transmission
16 is successfully received by T-1. However, T-1's reply is slow, and, at row 27, Port 500 is
17 released from its binding to L-1, and, at rows 28-29, is immediately grabbed by L-3 for an
18 ISAKMP-3 transmission. Thus, when T-1's ISAKMP-6 reply arrives at the gateway, as is
19 shown at rows 30 and 31, Port 500 is blocked, and the datagram is ignored. Thereafter,
20 L-1, not having received a reply to its ISAKMP-5 message, retransmits it at rows 34-35,
21 and a reply from T-1 is received at rows 36-37. Following their ISAKMP handshaking, L-1
22 and T-1 can communicate securely, using ESP protocol at rows 38-39 and 42-43.

1 Rows 38-57 of Figure 7 demonstrate the gateway's handling of a variety of
2 datagrams between a number of local computers and targets. UDP datagrams are shown
3 at rows 40-41, ESP datagrams at rows 42-43 and 52-53, and ISAKMP datagrams at rows
4 44-45. While the chart of Figure 7 shows different IP addresses for each device, in
5 practice it may occur that a number of processes will be running on the same device. The
6 substitution of unique source ports by the gateway, and the use of SPI's to differentiate
7 encrypted transmissions ensures that datagrams emanating from multiple processes
8 running on a single machine will not be misdirected.

9 Figure 8 depicts the initiation and transfer of signals between the datagram
10 processing circuitry 100 and the timer 110. Upon the occurrence of an event requiring a
11 port address to be bound to an IP address, a signal 120 will be sent to the timer to
12 commence timing. Upon the expiration of the appropriate interval, the timer will send a
13 signal 140 indicating that time has expired, in which case any port that is bound will be
14 released. In the interim, if an expected datagram has arrived, and a previously bound port
15 is to be released, a disabling signal 130 will be sent to the timer indicating that the timer
16 should be reset to await the next signal to begin timing. Obviously, there are numerous
17 timing circuits known in the art, and the specific configuration shown in Figure 8 is only one
18 of many possible embodiments.

19 From the foregoing it will be understood by those of skill in the art that the preferred
20 embodiment described herein is not the only means for practicing the invention, and that
21 other embodiments may be chosen to practice the invention without departing from the
22 spirit and scope of the invention. For example, although the preferred embodiment is
23 described with reference to Port 500, which has been reserved exclusively for use with the

1 ISAKMP protocol, the invention may be employed in the same manner for processing
2 datagrams destined for other port addresses that may in the future be assigned to other
3 processes or protocols. In particular, many games played over the internet require the use
4 of specific ports on local and external machines that cannot withstand normal address
5 translation. Additionally, although the invention has been described primarily with respect
6 to communications between a private LAN and the internet, it will be apparent that the
7 gateway of this invention can be used at any interface between two networks and will have
8 the same functionality as has been described.

9 The claims appended hereto are meant to cover modifications and changes within
10 the spirit and scope of the present invention.

11 What is claimed is:

CLAIMS

1. A network address translating gateway connecting a LAN to an external network, said LAN using local IP addresses, said gateway having a local IP address that can be seen by devices on said LAN and having an external IP address that can be seen by devices on said external network, said gateway comprising

a plurality of internal tables associating combinations of local IP addresses of local devices on said LAN, external IP addresses of external devices on said external network, SPI-In values, SPI-Out values, source port addresses, destination port addresses, reserved port addresses, and maintaining a list of reserved port addresses,

means for performing normal address translation upon datagrams passing from said LAN to said external network and datagrams passing from said external network to said LAN,

means for delivering a datagram from a local device on said LAN to an external device on said external network by receiving a datagram from a local device on said LAN intended for delivery to an external device on said external network, and determining whether said datagram is encrypted and, if said datagram is encrypted, for determining whether the SPI of said datagram is recorded in the SPI-Out field in said internal table and, if said SPI is recorded in said SPI-Out field, modifying the source IP address of said datagram to be said external IP address of said gateway and passing said datagram to said external network for routing and delivery to said external device,

and if said SPI is not recorded in said SPI-Out field of said internal table, setting the SPI-In field corresponding to the local IP address of said local device equal to zero and setting said SPI-Out field equal to said SPI, modifying said source IP address of said

1 datagram to be said external IP address of said gateway and passing said datagram to
2 said external network for routing and delivery to said external device,

3 and if said datagram is not encrypted, determining whether the destination port
4 address for said datagram is included in said list of reserved port addresses and, if said
5 destination port address is not included in said list of reserved port addresses, performing
6 normal address translation upon said datagram and passing said datagram to said external
7 network for routing and delivery to said external device,

8 and if said destination port address is included in said list of reserved port
9 addresses, determining whether said destination port address is bound to said local IP
10 address of said local device, and if said destination port address is bound to said local IP
11 address, performing normal address translation upon said datagram and passing said
12 datagram to said external network for routing and delivery to said external device,

13 and if said destination port address is not bound to said local IP address of said
14 local device, modifying said source IP address of said datagram to be said external IP
15 address of said gateway, binding said destination port address to said local IP address of
16 said local device and creating an association between said destination port address and
17 the external IP address of said external device, and passing said datagram to said external
18 network for routing and delivery to said external device,

19 means for delivering a datagram from said external device to said local device by
20 receiving a datagram from said external device on said external network intended for
21 delivery to said local device on said LAN,

22 determining whether said datagram is encrypted and, if said datagram is encrypted,
23 determining whether the datagram's SPI is recorded in said SPI-In field of said internal

1 table and, if said SPI is recorded in said SPI-In field, modifying the destination IP address
2 of said datagram to be said local IP address of said local device and passing said
3 datagram to said LAN for routing and delivery to said local device,

4 and if said SPI is not recorded in said SPI-In field of said internal table, determining
5 whether said SPI-In field corresponding to said IP address of said external device is equal
6 to zero and, if said SPI-In field is not equal to zero, discarding said datagram,

7 and if said SPI-In field is equal to zero, setting said SPI-In field equal to said SPI,
8 modifying the destination IP address of said datagram to be said local IP address of said
9 local device and passing said datagram to said LAN for delivery to said local device,

10 and if said datagram is not encrypted, determining whether the destination port
11 address for said datagram is included in said list of reserved port addresses and, if said
12 destination port address is not included in said list of reserved port addresses, performing
13 normal address translation upon said datagram and passing said datagram to said LAN
14 for delivery to said local device,

15 and if said destination port address is included in said list of reserved port
16 addresses, determining whether said destination port address is bound to the local IP
17 address of said local device, if said destination port address is not bound to said local IP
18 address, discarding said datagram,

19 and if said destination port address is bound to said local IP address, modifying said
20 destination IP address of said datagram to be said local IP address of said local device,
21 unbinding said destination port address from said local IP address, and passing said
22 datagram to said LAN for delivery to said local device.

1 2. The network address translating gateway of claim 1, further comprising a
2 timer, wherein, upon receiving a signal that a port address has become bound to an IP
3 address, said timer will commence timing for a predetermined length of time and, upon the
4 expiration of said predetermined length of time, will send a signal causing said port address
5 to become unbound from said IP address, and, upon receiving a signal indicating that said
6 port address has become unbound from said IP address prior to the expiration of said
7 predetermined length of time, said timer will stop timing and will reset.

8 3. The network address translating gateway of claim 1 in which said external
9 network is the internet.

10 4. The network address translating gateway of claim 3 in which said LAN is a
11 virtual private network.

12 5. A method of processing IP datagrams from a local device on a LAN using
13 local IP addresses through a network translating gateway to an external device on an
14 external network comprising the steps of

15 maintaining a plurality of tables associating local IP addresses of local devices on
16 said LAN, external IP addresses of external devices on said external network, port
17 addresses of said local devices, port addresses of said external devices, SPI-in values,
18 SPI-out values, and reserved port addresses, and a list of reserved port addresses,

19 receiving a datagram from said LAN

20 determining whether said datagram is encrypted and, if said datagram is encrypted,
21 determining whether the SPI in said datagram is recorded in the SPI-out field of one of said
22 plurality of internal tables and, if said SPI is recorded in said SPI-out field of said internal
23 table, modifying the source IP address to be the external IP address of said gateway and

1 passing said datagram to said external network for routing and delivery to said external
2 device,

3 and if said SPI is not recorded in said SPI-out field of said internal table, setting said
4 SPI-out field corresponding to the IP address of said external device equal to said SPI and
5 setting the SPI-in field of said internal table to zero, modifying said source IP address to
6 be said external IP address of said gateway, and passing said datagram to said external
7 network for routing and delivery to said external device,

8 and if said datagram is not encrypted, determining whether the destination port
9 address for said datagram is included in said table of reserved port addresses and, if said
10 destination port address is not included in said table of reserved port addresses,
11 performing normal address translation upon said datagram and passing said datagram to
12 said external network for routing and delivery to said external device,

13 and if said destination port address is included in said table of reserved port
14 addresses, determining whether said destination port address is bound to an IP address,
15 and if said destination port is bound to an IP address, performing normal address
16 translation upon said datagram and passing said datagram to said external network for
17 routing and delivery to said external device,

18 and if said destination port address is not bound to an IP address, modifying said
19 source IP address to be said external IP address for said external device, binding said
20 destination port address to the local IP address of said local device and creating an
21 association between said destination port address and said external IP address of said
22 external device, and passing said datagram to said external network for routing and
23 delivery to said external device.

1 6. A method of processing IP datagrams from an external device on an external
2 network through a network translating gateway to a local device on a LAN using local IP
3 addresses, comprising the steps of

4 maintaining a plurality of tables associating local IP addresses of local devices on
5 said LAN, external IP addresses of external devices on said external network, port
6 addresses of said local devices, port addresses of said external devices, SPI-in values,
7 SPI-out values, and reserved port addresses, and a list of reserved port addresses,

8 receiving a datagram from said external network

9 determining whether said datagram is encrypted and, if said datagram is encrypted,
10 determining whether the SPI in said datagram is recorded in the SPI-in field of one of said
11 plurality of internal tables and, if said SPI is recorded in said SPI-in field of said internal
12 table, modifying the destination IP address to be the internal IP address of said local
13 device and passing said datagram to said LAN for routing and delivery to said local device,

14 and if said SPI is not recorded in said SPI-in field of said internal table, determining
15 whether said SPI-in field corresponding to the IP address of said external device is zero,
16 and if said SPI-in field is not zero, discarding said datagram,

17 and if said SPI-in field is equal to zero, modifying said SPI-in field to be said SPI,
18 modifying said destination IP address to be said local IP address of said local device, and
19 passing said datagram to said LAN for routing and delivery to said local device,

20 and if said datagram is not encrypted, determining whether the destination port
21 address for said datagram is included in said list of reserved port addresses, and if said
22 destination port address is not included in said list of reserved port addresses, performing

1 normal address translation and passing said datagram to said LAN for routing and delivery
2 to said local device,

3 and if said destination port address is included in said list of reserved port
4 addresses, determining whether said destination port address is bound to said local IP
5 address, and if said destination port is not bound to said local IP address, discarding said
6 datagram,

7 and if said destination port address is bound to said local IP address, modifying said
8 destination IP address to be said local IP address of said local device, unbinding said
9 destination port address from said local IP address, and passing said datagram to said
10 LAN for routing and delivery to said local device.

11 7. The method of processing IP datagrams as claimed in claim 5, further
12 comprising the steps of starting a timer whenever said destination port address becomes
13 bound to said local IP address of said local device,

14 resetting said timer whenever said destination port address has become released,
15 and sending a signal whenever said timer is active and a predetermined length of
16 time has expired from the time said timer was started.

17 8. The method of processing IP datagrams as claimed in claim 6, further
18 comprising the steps of starting a timer whenever said destination port address becomes
19 bound to said local IP address of said local device,

20 resetting said timer whenever said destination port address has become released,
21 and sending a signal whenever said timer is active and a predetermined length of
22 time has expired from the time said timer was started.

1 9. The method of processing IP datagrams as claimed in claim 5, in which said
2 external network is the internet.

3 10. The method of processing IP datagrams as claimed in claim 6, in which said
4 external network is the internet.

5 11. The method of processing IP datagrams as claimed in claim 5 in which said
6 LAN is a virtual private network.

7 12. The method of processing IP datagrams as claimed in claim 6 in which said
8 LAN is a virtual private network.

ABSTRACT

A network address translation gateway provides normal network translation for IP datagrams traveling from a local area network using local IP addresses to an external network, but suspends source service address (port) translation when the port is reserved for a specific protocol, such as the ISAKMP "handshaking" protocol that is part of the IPSec protocol model. ISAKMP exchanges require both source and target computers to use the same service address (port). By providing a network interface that does not translate the source service address (port), this gateway enables the initiation and maintenance of secure, encrypted transmissions using IPSec protocol between a local area network using local IP addresses and servers on the internet.

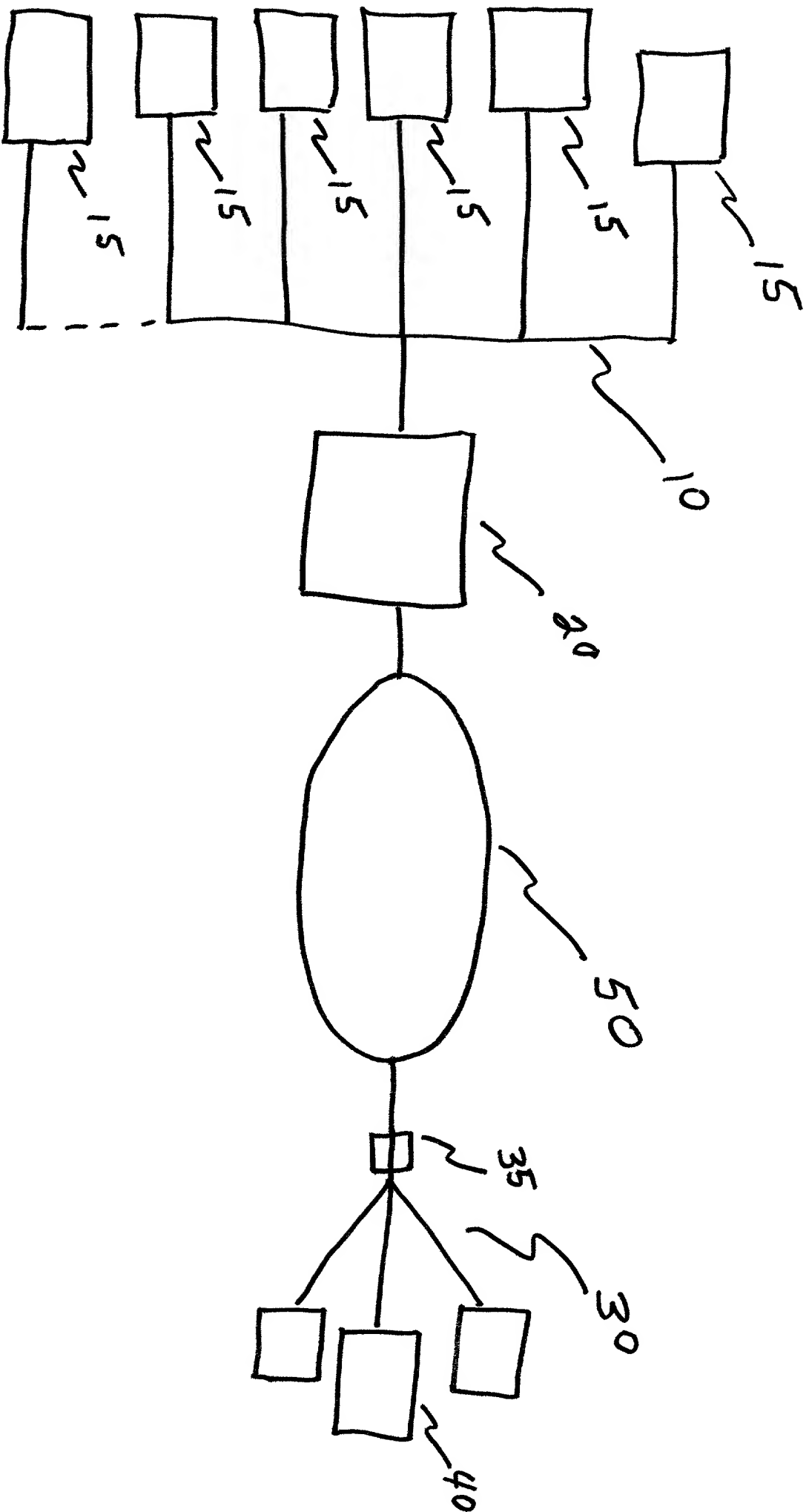


FIGURE 1

DECISION TREE FOR DATAGRAM FROM LAN

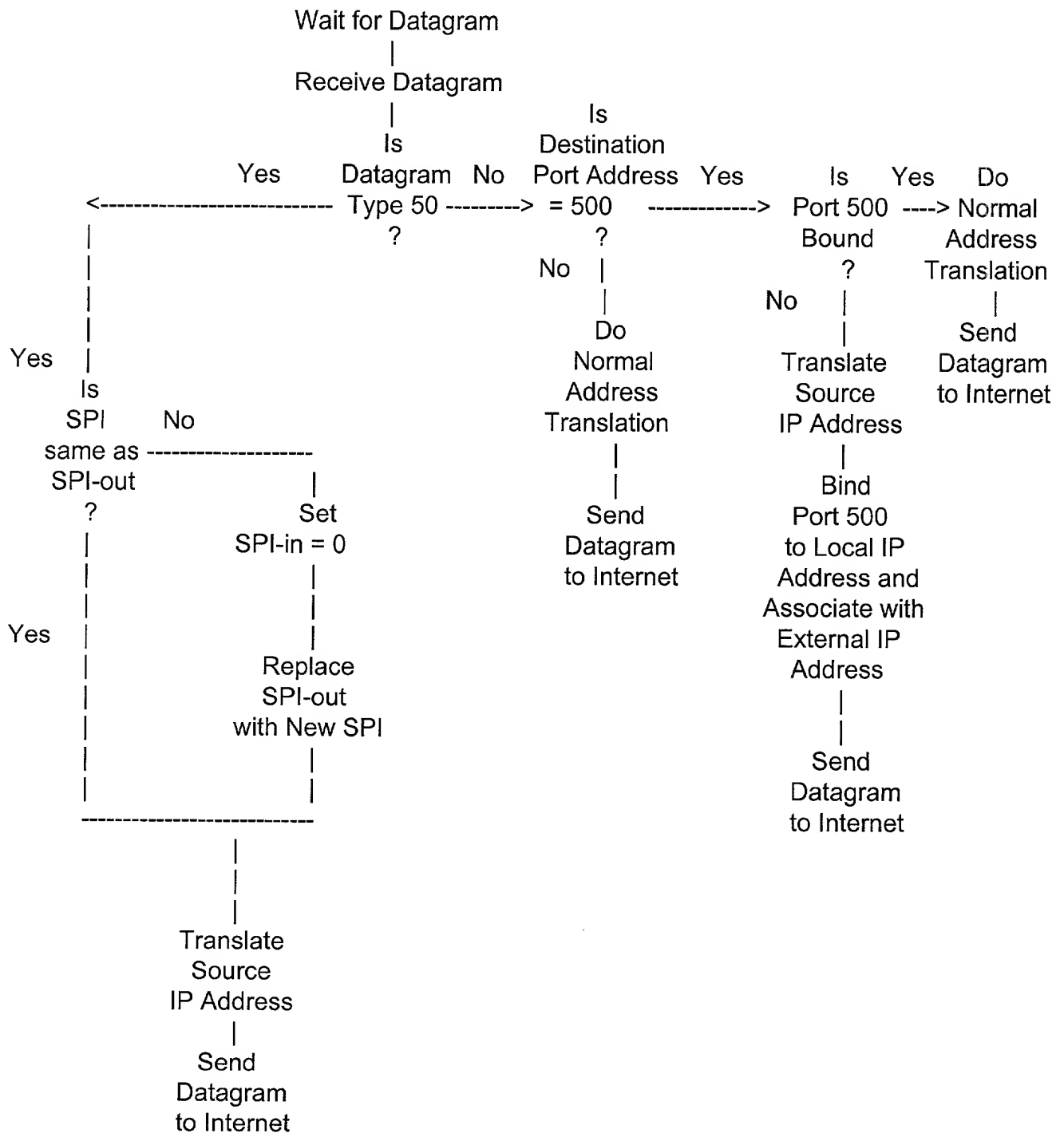


FIGURE 2

DECISION TREE FOR DATAGRAM FROM INTERNET

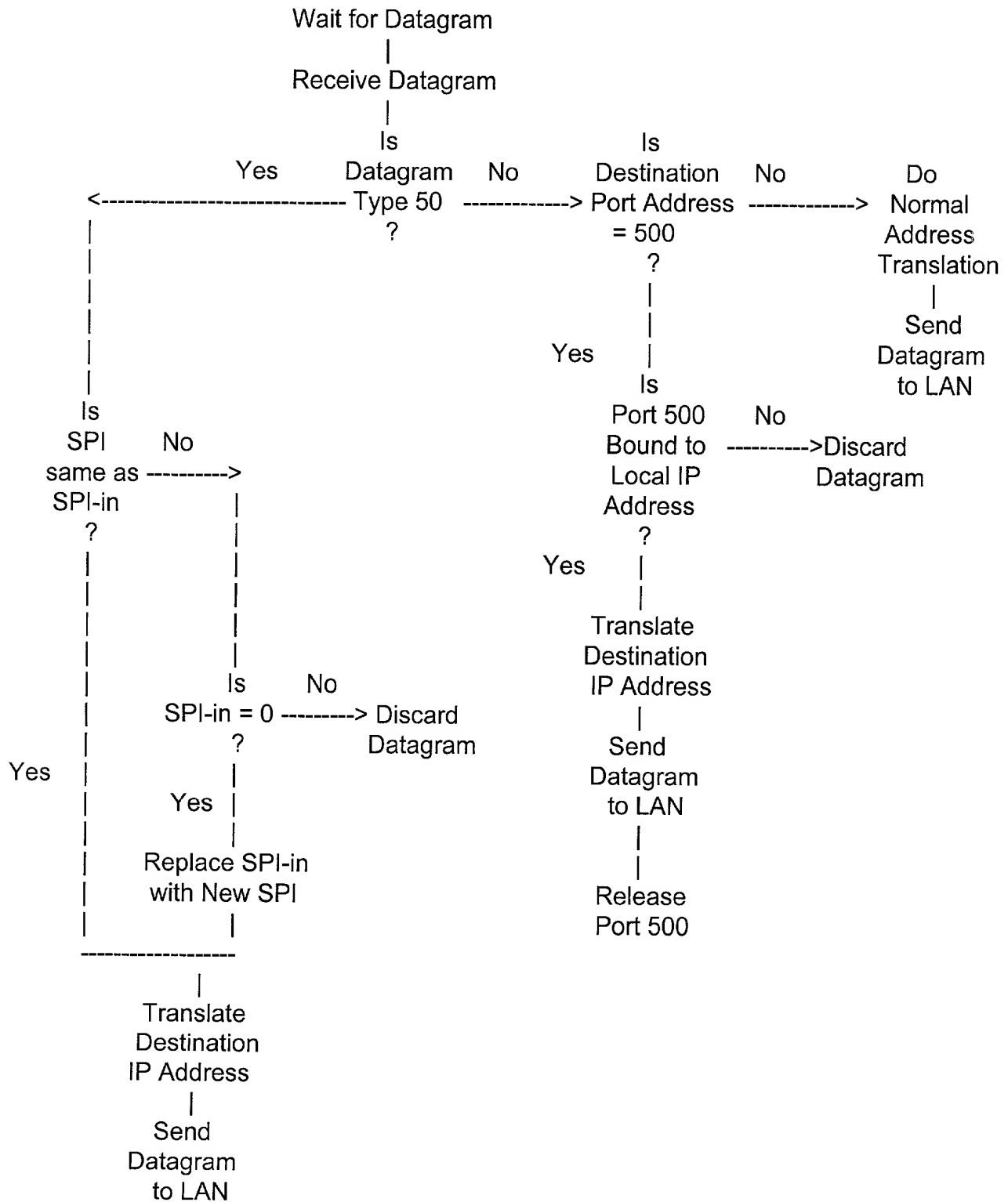


FIGURE 3

IP Addresses

	Local Computer	Gateway Internal	Gateway External	Target	
L-1	192.168.0.2	102.168.0.1	142.140.3.6	204.71.202.160	T-1
L-2	192.168.0.4	102.168.0.1	142.140.3.6	207.46.131.137	T-2
L-3	192.168.0.3	102.168.0.1	142.140.3.6	207.158.227.235	T-3

FIGURE 4

SPI table – 8 local computers communicating with 3 hosts

	TARGET	LOCAL IP		SPI-out	SPI-in
T-1	204.71.202.160	192.168.0.2	L-1	4859	9802
		192.168.0.5	L-x	52856	7000
		192.168.0.10	L-x	8565	8523
T-2	207.46.131.137	192.168.0.4	L-2	1353	6234
		192.168.0.7	L-x	2562	10125
		192.168.0.10	L-x	25763	12106
T-3	207.158.227.235	192.168.0.3	L-3	38935	7753
		192.168.0.8	L-x	9093	32828

FIGURE 5a

New session – new SPI-out – SPI-in set to 0

	TARGET	LOCAL IP		SPI-Out	SPI-In
T-1	204.71.202.160	192.168.0.2	L-1	14662	0
		192.168.0.5	L-x	52856	7000
		192.168.0.10	L-x	8565	8523
T-2	207.46.131.137	192.168.0.4	L-2	1353	4562
		192.168.0.7	L-x	2562	10125
		192.168.0.10	L-x	25763	12106
T-3	207.158.227.235	192.168.0.3	L-3	8773	20889
		192.168.0.8	L-x	9093	32828

FIGURE 5b

Reply packet received – New SPI-in received

	TARGET	LOCAL IP		SPI-OU	SPI-IN
T-1	207.200.0.2	192.168.0.2	L-1	14662	3288
		192.168.0.5	L-x	52856	7000
		192.168.0.10	L-x	8565	8523
T-2	206.23.5.120	192.168.0.4	L-2	1353	6234
		192.168.0.7	L-x	43966	17937
		192.168.0.10	L-x	25763	12106
T-3	207.198.75.3	192.168.0.3	L-3	8773	20889
		192.168.0.8	L-x	9093	32828

FIGURE 5c

SEQUENCE OF PACKETS THROUGH GATEWAY SINGLE LOCAL MACHINE -- SINGLE TARGET						
Path	Datagram Type	Source Address IP Port		Destination Address IP Port		SPI
						Row
LAN - Gate	UDP	192.168.0.2	6404	204.71.202.160	80	1
Gate - Net	UDP	142.140.3.6	10425	204.71.202.160	80	2
Net - Gate	UDP	204.71.202.160	80	142.140.3.6	10425	3
Gate - LAN	UDP	204.71.202.160	80	192.168.0.2	6404	4
LAN - Gate	ISAKMP-1	192.168.0.2	500	204.71.202.160	500	5
Gate - Net	ISAKMP-1	142.140.3.6	500	204.71.202.160	500	6
Net - Gate	ISAKMP-2	204.71.202.160	500	142.140.3.6	500	7
Gate - LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500	8
LAN - Gate	ISAKMP-3	192.168.0.2	500	204.71.202.160	500	9
Gate - Net	ISAKMP-3	142.140.3.6	500	204.71.202.160	500	10
Net - Gate	ISAKMP-4	204.71.202.160	500	142.140.3.6	500	11
Gate - LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500	12
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500	13
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500	14
Net - Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500	15
Gate - LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500	16
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		14662
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		14662
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		3288
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		3288
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		14662
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		14662
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		3288
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		3288

FIGURE 6

SEQUENCE OF PACKETS THROUGH GATEWAY							
MULTIPLE LOCAL MACHINES -- MULTIPLE TARGETS							
Path	Packet Type	Source Address		Destination Address		SPI	Active Process
		IP	Service	IP	Service		
LAN - Gate	UDP	192.168.0.2	6404	204.71.202.160	80		L-1 Out
Gate - Net	UDP	142.140.3.6	10425	204.71.202.160	80		T-1 In
LAN - Gate	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 Out
Gate - Net	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 In
Net - Gate	UDP	204.71.202.160	80	142.140.3.6	10425		T-1 Out
Gate - LAN	UDP	204.71.202.160	80	192.168.0.2	6404		L-1 In
Net - Gate	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 Out
Gate - LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 In
LAN - Gate	ISAKMP-1	192.168.0.2	500	204.71.202.160	500		L-1 Out -- Port 500 bound to 192.168.0.
Gate - Net	ISAKMP-1	142.140.3.6	500	204.71.202.160	500		T-1 In -- Associated with 204.71.202.160
Net - Gate	ISAKMP-2	204.71.202.160	500	142.140.3.6	500		T-1 Out
Gate - LAN	ISAKMP-2	204.71.202.160	500	192.168.0.2	500		L-1 In -- Port 500 released
LAN - Gate	ISAKMP-3	192.168.0.2	500	204.71.202.160	500		L-1 Out -- Port 500 bound to 192.168.0.
Gate - Net	ISAKMP-3	142.140.3.6	500	204.71.202.160	500		T-1 In -- Associated with 204.71.202.160
LAN - Gate	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 Out
Gate - Net	ISAKMP-1	142.140.3.6	500	207.158.227.235	8773		T-3 In - Port 500 not available
Net - Gate	ISAKMP-4	204.71.202.160	500	142.140.3.6	500		T-1 Out
Gate - LAN	ISAKMP-4	204.71.202.160	500	192.168.0.2	500		L-1 In -- Port 500 released
LAN - Gate	ISAKMP-1	192.168.0.3	500	207.158.227.235	500		L-3 Out
Gate - Net	ISAKMP-1	142.140.3.6	500	207.158.227.235	500		T-3 In - Port 500 bound to 192.168.0.3
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out -- Port 500 not available
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	9063		T-1 In -- Source port address translated
Net - Gate	ISAKMP-2	207.158.227.235	500	142.140.3.6	500		T-3 Out
Gate - LAN	ISAKMP-2	207.158.227.235	500	192.168.0.3	500		L-3 In -- Port 500 released
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out -- Port 500 bound to 192.168.0.
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 In -- Associated with 204.71.202.160
							Time-out for T-1 Out--Port 500 released
LAN - Gate	ISAKMP-3	192.168.0.3	500	207.158.227.235	500		L-3 Out
Gate - Net	ISAKMP-3	142.140.6.3	500	207.158.227.235	500		T-3 In - Port 500 bound to 192.168.0.3
Net - Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 Out -- Port 500 blocked
							T-1 Out -- packet ignored
Net - Gate	ISAKMP-4	207.158.227.235	500	142.140.3.6	500		T-3 Out
Gate - LAN	ISAKMP-4	207.158.227.235	500	192.168.0.3	500		L-3 In -- Port 500 released
LAN - Gate	ISAKMP-5	192.168.0.2	500	204.71.202.160	500		L-1 Out -- Port 500 bound to 192.168.0.
Gate - Net	ISAKMP-5	142.140.3.6	500	204.71.202.160	500		T-1 In -- Associated with 204.71.202.160
Net - Gate	ISAKMP-6	204.71.202.160	500	142.140.3.6	500		T-1 Out
Gate - LAN	ISAKMP-6	204.71.202.160	500	192.168.0.2	500		L-1 In -- Port 500 released

Figure 7 (Page 1)

LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859	L-1 Out	38
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859	T-1 In	39
LAN - Gate	UDP	192.168.0.4	4562	207.46.131.137	1353		L-2 Out	40
Gate - Net	UDP	142.140.3.6	37525	207.46.131.137	1353		T-2 In	41
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802	T-1 Out	42
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	L-1 In	43
LAN - Gate	ISAKMP-5	192.168.0.3	500	207.158.227.235	500		L-3 Out - Port 500 bound to 192.168.0.3	44
Gate - Net	ISAKMP-5	142.140.6.3	500	207.158.227.235	500		T-3 In - Associated with 207.158.227.23	45
LAN - Gate	ESP (50)	192.168.0.2		204.71.202.160		4859	L-1 Out	46
Gate - Net	ESP (50)	142.140.3.6		204.71.202.160		4859	T-1 In	47
Net - Gate	ISAKMP-6	207.158.227.235	500	142.140.3.6	500		T-3 Out	48
Gate - LAN	ISAKMP-6	207.158.227.235	500	192.168.0.3	500		L-3 In - Port 500 released	49
Net - Gate	UDP	207.46.131.137	1353	142.140.3.6	37525		T-2 Out	50
Gate - LAN	UDP	207.46.131.137	1353	192.168.0.4	4562		L-2 In	51
LAN - Gate	ESP (50)	192.168.0.3		207.158.227.235		38935	L-3 Out	52
Gate - Net	ESP (50)	142.140.6.3		207.158.227.235		38935	T-3 In	53
Net - Gate	ESP (50)	204.71.202.160		142.140.3.6		9802	T-1 Out	54
Gate - LAN	ESP (50)	204.71.202.160		192.168.0.2		9802	L-1 In	55
Net - Gate	ESP (50)	207.158.227.235		142.140.3.6		7753	T-3 Out	56
Gate - LAN	ESP (50)	207.158.227.235		192.168.0.3		7753	L-3 In	57

Figure 7 (Page 2)

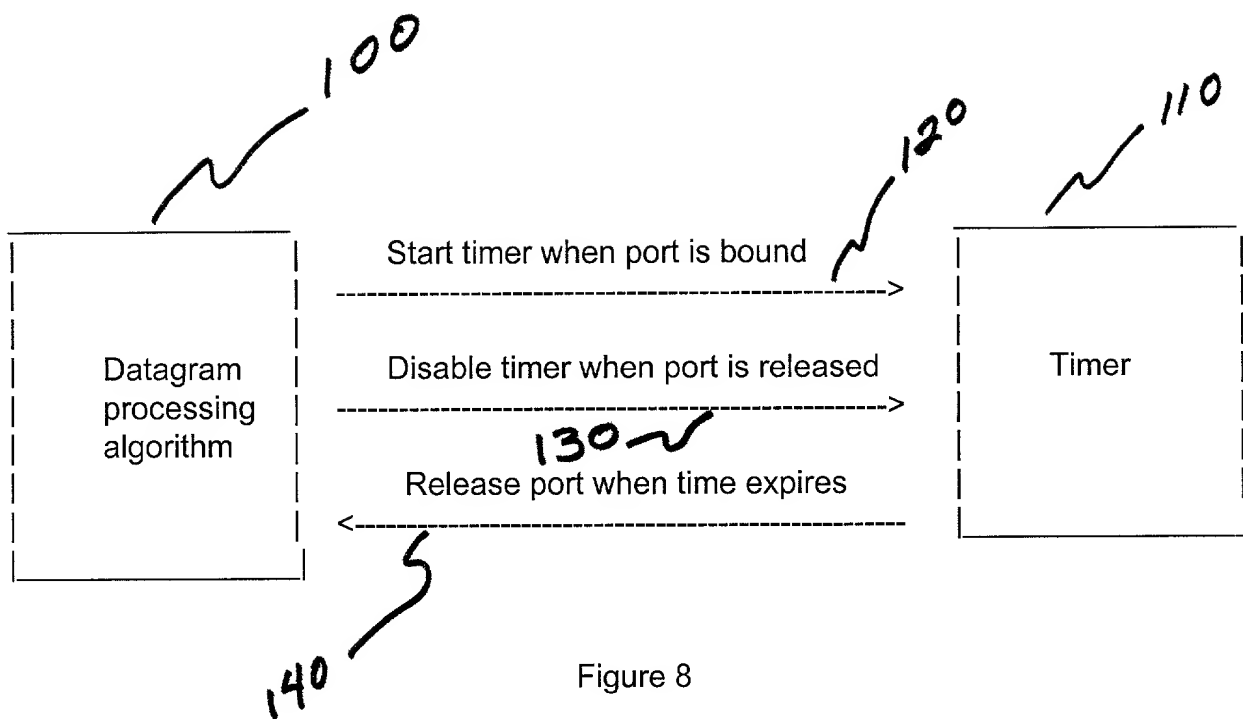


Figure 8

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled NETWORK ADDRESS TRANSLATION GATEWAY FOR LOCAL AREA NETWORKS USING LOCAL IP ADDRESSES AND NON-TRANSLATABLE PORT ADDRESSES the specification of which

(check one)



is attached hereto.



was filed on _____

as Application Serial No. _____

and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56(a).

I hereby claim foreign priority benefits under Title 35, United States Code, §119 (a-d) or §365(b) of any foreign application(s) for patent or inventor's certificate, or §365(a) of any PCT international application which designated at least one country other than the United States of America, listed below and have also identified below any foreign application for patent or inventor's certificate, or any PCT international application having a filing date before that of the application on which priority is claimed:

Prior Foreign Application(s)

Priority Claimed

(Number)

(Country)

(Day/Month/Year Filed)



Yes



No

(Number)

(Country)

(Day/Month/Year Filed)



Yes



No

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56(a) which occurred between the filing date of the prior application and the national or PCT international filing date of this application:

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)
(patented, pending, abandoned)

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

(Provisional Application No.)

(Filing Date)

(Provisional Application No.)

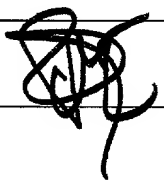
(Filing Date)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agents to prosecute this application and transact all business in the Patent and Trademark Office connected therewith.
Michael C. Cesarano, Reg. No. 31,817.

Send Correspondence to: Michael C. Cesarano
Bienstock & Clark
200 So. Biscayne Boulevard, Suite 3160
Miami, Florida 33131

Direct Telephone Calls to: Michael C. Cesarano, (305) 373-1100

Israel Daniel Sultan	
Full name of <u>sole or first inventor</u>	
/	
Inventor's signature	Date
Paris, France	03/01/2000
Residence	
French	
Citizenship	
9 Rue Caillaux, 75013 Paris - FRANCE	
Post Office Address	
Full name of <u>second joint inventor, if any</u>	
Inventor's signature	Date
Residence	
Citizenship	
Post Office Address	
(Supply similar information and signature for third and subsequent joint inventors.)	